International Journal of Mathematics and Computer Science
Volume **20,** Issue no. 1, (2025), 435–438
DOI: https://doi.org/10.69793/ijmcs/01.2025/sukaina

A New High-Performance Public-Key Encryption Scheme Using Two Algebras

Sukaina Abdullah Al-Bairmani[1], **Najwan Noori Hani**[2], **Hassan Rashed Yassein**[3]

[1]Department of Mathematics
College of Basic Education
University of Babylon
Hillah, Iraq

[2]Department of Chemistry
College of Education
University of Al-Qadisiyah
Al-Qadisiyah, Iraq

[3]Department of Mathematics
College of Education
University of Al-Qadisiyah
Al-Qadisiyah, Iraq

email: sukaina.albairmani@uobabylon.edu.iq, najwan.noori@qu.edu.iq, hassan.yaseen@qu.edu.iq

(Received November 7, 2024, Accepted December 8, 2024, Published December 12, 2024)

Abstract

In this work, we present an asymmetric encryption system using the quaternion algebra of truncated polynomials whose coefficients are in the KAH-Octo algebra. This system gives high performance in terms of the level of security for both key and message, providing encrypted text that is difficult to hack by hackers on the transmission medium.

Key words and phrases: Quaternion algebra, KAH-Octo algebra, NTRU.
AMS (MOS) Subject Classifications: 94A60.
ISSN 1814-0432, 2025, https://future-in-tech.net

1 Introduction

The NTRU method is one of the important methods in encryption that is used in various fields [1]. In 2008, Malecian et al. [2] presented an improvement to the QTRU based on the quaternion algebra. In 2021, Abo-Alsood and Yassein [3] proposed an improvement to the NTRU called QOTRU through the Qu-Octonion algebraic structure. In 2022 Abo-Alsood and Yassein [4] proposed an improvement called TOTRU by employing the octonion algebra in the mathematical construction process. In 2023, Yassein et al. [5] presented a system similar to the NTRU, called QuiTRU, based on a new mathematical structure with a five-dimensional algebraic structure.

2 Proposed KPNTR Cryptosystem

A new public key cryptosystem KPNTR depends on para-quaternion [6] with coefficients in KAH-Octo (KO) [7] with the same parameters in NTRU. Consider a finite ring χ with characteristics not equal 2, define para quaternion algebra Γ over KO as follows: $\Gamma = \{\sigma+\alpha i+\beta j+\gamma k \mid \delta,\ \alpha,\ \beta, \gamma \in \chi\}$. Take the rings of truncated polynomials $\zeta = \frac{Z[x]}{(x^N-1)}, \zeta_p(x) = Z_p[x]/xN-1 and \zeta_{\mathfrak{q}}(x) = Z_{\mathfrak{q}}[x]/xN-1$.

Define three para-quaternion algebras η, η_p, and $\eta_{\mathfrak{q}}$ as follows:

$$\eta = \{f_0(x) + f_1(x)i + f_2(x)j + f_3(x)k \mid f_0,\ f_1,\ f_2, f_3 \in \zeta\}.$$

$$\eta_p = \{f_0(x) + f_1(x)i + f_2(x)j + f_3(x)k \mid f_0,\ f_1,\ f_2, f_3 \in \zeta_p\},$$

$$\eta_{\mathfrak{q}} = \{f_0(x) + f_1(x)i + f_2(x)j + f_3(x)k \mid f_0,\ f_1,\ f_2, f_3 \epsilon\ \zeta_{\mathfrak{q}}\}.$$

Subsets $\iota_F,\ \iota_G,\ \iota_M$ and $\iota_V \subset \eta$ where $\iota_F = \{\sum_{\tau=0}^{7} f_{0\tau}(x)\cdot\beta_\tau + \sum_{\tau=0}^{7} f_{1\tau}(x)\cdot\beta_\tau i + \sum_{\tau=0}^{7} f_{2\tau}(x)\cdot\beta_\tau j + \sum_{\tau=0}^{7} f_{3\tau}(x)\cdot\beta_\tau k | f_{\tau c}(x)$ has d_f coefficients equal to $+1$, $d_f - 1$ equal to -1, remaining coefficients are 0, $c = 0,1,2,3\}$, $\iota_G = \{\sum_{\tau=0}^{7} g_{0\tau}(x)\cdot\beta_\tau + \sum_{\tau=0}^{7} g_{1\tau}(x)\cdot\beta_\tau i + \sum_{\tau=0}^{7} g_{2\tau}(x)\cdot\beta_\tau j + \sum_{\tau=0}^{7} g_{3\tau}(x)\cdot\beta_\tau k | g_{\tau c}(x)$ has d_g coefficients equal to $+1, d_g$ equal to -1, remaining coefficients are $0, c = 0,1,2,3\}$, $\iota_M = \{\sum_{\tau=0}^{7} m_{0\tau}(x).\beta_\tau + \sum_{\tau=0}^{7} m_{1\tau}(x).\beta_\tau i + \sum_{\tau=0}^{7} m_{2\tau}(x).\beta_\tau j + \sum_{\tau=0}^{7} m_{3\tau}(x).\beta_\tau k | m_{\tau c}(x)$ with coefficients in $(-\frac{p}{2}, \frac{p}{2}], c = 0,1,2,3\}$, and ι_V defined as ι_f.

The KPNTR method is described in the following phases:

I. **Key generate:** The recipient chooses two private keys F and G from subsets ι_F and ι_G, respectively, to generate the public key $\mathcal{H}$ in the

following formula: $\mathcal{H} = F^{-1} * G \ mod \ \mathfrak{q}$. This means that each of the keys F and G consists of 32 keys inside it and thus the total number of private keys is 64.

II. **Encryption:** After the sender receives the public key $\mathcal{H}$ from the sender to start the process of encrypting the original message M, performs the following steps:
- Convert the message into the form of elements ι_M
- Choose a private key $\mathcal{V} \in \iota_V$
- Calculate the encrypted text $\mathfrak{E}$ by the following formula:

$$\mathfrak{E} = p\mathcal{H} * \mathcal{V} + M \ mod \ \mathfrak{q} with coefficients belong to \left(\frac{-\mathfrak{q}}{2}, \ \frac{\mathfrak{q}}{2} \right].$$

III. **Decryption:** After the encrypted text is received and the sender obtains the plaintext, he\she takes the following steps:

After the recipient receives the encrypted message $\mathfrak{E}$, the purpose of converting it into understandable text is to take several steps to achieve this, as follows:
- Compute $F * \mathfrak{E} \ \ (mod \ \mathfrak{q}) \equiv F * (\ p\mathcal{H} * \mathcal{V} + M) \ mod \ \mathfrak{q}$
$\equiv F * \big(p(F^{-1} * G) * \ \mathcal{V} + M) \ mod \ \mathfrak{q} \equiv \ p(F * F^{-1}) * G) * \mathcal{V} + F * M mod \ \mathfrak{q}$
$\equiv pG * \mathcal{V} + F * M \ mod \ \mathfrak{q}$, such that the coefficients belong to $\left(\frac{-\mathfrak{q}}{2}, \ \frac{\mathfrak{q}}{2}\right]$.

Now, convert $pG * \mathcal{V} + F * M$ from $mod \ \mathfrak{q}$ to $mod \ p$, therefore $pG * \mathcal{V} + F * M \ mod \ p \ \equiv F * M \ mod \ p$. Thus, $M \equiv (F^{-1} * F) * M \ mod \ p$, with coefficients belong to $\left(\frac{-p}{2}, \ \frac{p}{2}\right]$.

3 Brute Force Attack

In order for the attacker to be able to decrypt the encrypted text through a brute force attack, he/she must go in one of two ways. The first is by accessing the thirty-two private keys that make up the public key G (Assuming that the space of G is less than F) and with $\left(\frac{N!}{(d_g!)^2(N-2d_g)!}\right)^{32}$ attempts. The second is to know the keys that make up the private key in the encryption phase and with $\left(\frac{N!}{(d_v!)^2(N-2d_v)!}\right)^{32}$ attempts for the need to know thirty-two keys.

4 Conclusions

The KPNTR method is considered a multidimensional method due to the multidimensional algebra used in its construction, which contributed to increasing the level of security for private keys, whether in the key generation phase or the encryption phase. This gives a high level of security to the new method, which contributes to its effectiveness in many transactions that are exposed to attacks by hackers, especially financial and military transactions.

References

[1] J. Hoffstein, J. Pipher, J. H. Silverman, NTRU: A ring-based public key cryptosystem. In Algorithmic Number Theory, Proceedings Third International Symposium, (1998), 267–288.

[2] E. Malecian, A. Zakerolhsooeini, A. Mashatan, QTRU: Quaternionic Version of the NTRU Public-Key Cryptosystems, The ISC International Journal of Information Security, **3,** no. 1, (2011), 29–42.

[3] H. H. Abo-Alsood, H. R. Yassein, QOTRU: A New Design of NTRU Public Key Encryption Via Qu-Octonion Subalgebra, Journal of Physics: Conference Series, 1999, no. 1, (2021), 1–7.

[4] H. H. Abo-alsood, H. R. Yassein, Analogue to NTRU public key cryptosystem by multi-dimension algebra with high security, AIP Conference Proceedings, 2386, (2022), 600091–600096.

[5] H. R. Yassein, H. N. Zaky, H. H. Abo-Alsoo, I. A. Mageed, W. I. El-Sobky, QuiTRU: Design Secure Variant of Ntruencrypt Via a New Multi-Dimensional Algebra, Applied Mathematics & Information Sciences, **17,** no. 1, (2023), 1–5.

[6] N. Blazic, Paraquaternionic projective space and pseudo-Riemannian geometry, Publ. Inst. Math.(Beograd)(NS), **60,** no. 74, (1996), 101–107.

[7] K. A. Hassoon, H. R. Yassein, Proposed Multi-Dimensional Algebra, International Journal of Mathematics and Computer Science, **19,** no. 3, (2024), 765–770.